98

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,583	05/16/2001	Ikuya Morikawa	FUJA 18.671	9888

26304 7590 04/20/2006

KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/863,583	**Applicant(s)** MORIKAWA ET AL.	
	Examiner Thanhnga B. Truong	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/27/2006 (RCE)*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 May 2001* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 27, 2006 has been entered. Claims 1, 3-28 are pending and claim 2 is cancelled by the applicant.

Claim Objections

2. Claims 1, 4, 5, 6 objected to because of the following informalities:

a. _Referring to claim 1:_

i. A colon (:) is missing after the words "provided with" in the pre-amble section of the claim 1. Also, a comma is missing between the words "request and" on line 7 of claim 1. Appropriate correction is required.

b. _Referring to claim 4:_

i. A colon (:) is missing after the words "comprised of" in the pre-amble section of the claim 4. Since the applicant is using a format of "a first step for processing", then the rest of the limitations in this method of claim should be the same, such as "a second step for", "a third step for", etc. Appropriate correction is required.

c. _Referring to claim 5:_

i. A colon (:) is missing after the words "provided with" in the pre-amble section of the claim 5. Appropriate correction is required.

d. _Referring to claim 6:_

i. A colon (:) is missing after the words "for every group, including" in the pre-amble section of the claim 6. Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 3-7, 10-14, 17-18, 21-25, 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mashayekhi (US 5,818,936), further in view of Ohashi et al (US 5,761,309), and further in view of Hamann (US 6,981,147 B1).

a. *Referring to claim 1:*

i. Mashayekhi teaches a system of distributed group management for indirectly authenticating membership of a user in a group in order to manage security for a client on a client side and a server for executing a remote processing request from the client side under a predetermined authorization assigned for every group (column 3, lines 25-53), provided with:

(1) a group certificate issuing apparatus for issuing a group certificate on the client side based on original group information including the name of the group to which the related user belongs. when there is said remote processing request **[i.e. referring to Figure 2, element 220 function is to generate a certificate with username/groupname and crypto key binding together (column 5, lines 34-55 of Mashayekhi)]**; and

(2) a group certificate verification unit for verifying a legitimacy of said group certificate transmitted from the client side in said server, wherein said group certificate issuing apparatus adds an issuance side processed value obtained by encrypting the information of the original group information by a cryptographic function to the original group information and defines this as the group certificate **[i.e., referring to Figure 2 again, when the authentication inquiry is received at the controller, the workstation API 214 verifies that the user is a valid network client (i.e., has successively logged-on and has been authenticated to the NDS) by requesting the proper application secret for program 236. In**

response to this latter request, the database API 206 accesses the authentication database 204 and provides an encrypted application secret along with the private key for decrypting the secret. The workstation API then decrypts and forwards the proper application secret (and user identity) to the particular application program (column 6, lines 60-67 through column 7, lines 1-27). Accordingly, to effect a secure transmission of information to a recipient, a principal encodes ("encrypts") the information with the recipient's public key. Since only the intended recipient has the complementary private key, only that principal can decode ("decrypt") it. On the other hand, to prove to a recipient of information that the sender is who he purports to be, the sender encodes ("signs") the information with its private key. If the recipient can decode ("verify") the information, it knows that the sender has correctly identified itself (column 1, lines 51-60). In addition, the group of encrypted application secrets associated with the user is referred to as a "keychain." Each keychain is assigned a public/private key pair, with all secrets in the keychain being encrypted with the public key (column 3, lines 40-43 of Mashayekhi)],

(3) said group certificate verification unit processes part of the information included in the received group certificate by an identical cryptographic function to obtain a verification side processed value and performs said authentication by confirming that said issuance side processed value and said verification side processed value coincide **[i.e., Figures 4A and 4B are a flow chart of the function performed by workstation API 214 in response to the authentication request generated by a particular program. As noted, when a user 201 attempts to access a particular application program, such as a local application 240 or network-based application program 236, the particular application program requires that the user be authenticated prior to accessing its processes or data. The function begins at block 400 and proceeds to block 402 where workstation API 214 receives this authentication inquiry from the application program. Upon receipt, the workstation API 214 determines whether the user is a valid network client at block 404. If the user is not a valid network client, workstation API 214 denies the**

user access to the distributed authentication service at block 406. However, if the user is a valid network client, then the workstation API 214 requests the proper application secret for the particular application program at block 410. For example, the workstation API 214 calls a "Retrieve Application Secret" API for retrieving the user's identity and proper application secrets. Workstation API 214 provides the application identifier of the particular application as part of the API call. The request to the database API 206 is preferably encoded in a network protocol element in a matter that is well-known in the art. The database API 206, in a matter described below with reference to Figure 5, returns encrypted data and a keychain private key to the workstation API 214. At block 414, the workstation API 214 receives the encrypted data and keychain private key (column 7, lines 10-38 of Mashayekhi)],

(4) said group certificate issuing apparatus includes first secret information assigned to said groups in said original group information and performs the processing by said cryptographic function, said first secret information being held only by said group certificate issuing apparatus **[i.e., the group of encrypted application secrets associated with the user is referred to as a "keychain." Each keychain is assigned a public/private key pair, with all secrets in the keychain being encrypted with the public key. The user may be associated with one or more keychains, each of which may be further associated with different secrets (e.g. first secret, second secret, etc...). Since these secrets correspond to application programs, the association of programs to keychains may be based upon various characteristics, such as the user's rights with respect to the programs. Furthermore, each application program may be accessible by the same or different users so that, e.g., those users having the same access rights for a program may utilize the same keychain containing each user's secrets for the programs (column 3, lines 40-53 of Mashayekhi). Furthermore, referring to Figure 1, a distributed data processing network system 100 includes a plurality of computer nodes, such as user nodes 102a-n and various server nodes 104a-n, interconnected by a communications medium 106. The user node, e.g., a**

workstation 102a, is a computer generally configured for use by one user at a time, whereas each server 104 is a computer resource running specialized software applications and services, typically for use by many users. In general, each of the computer nodes includes memory means 108 for storing software programs and data structures associated with the cryptographic methods and techniques described herein (column 4, line 61-67 through column 5, lines 1-5 of Mashayekhi)],

(5) said group certificate verification unit includes second secret information assigned to the groups in part of information included in said received group certificate and performs the processing by said cryptographic function, said second secret information being held only by said group certificate verification unit, and said first secret information and said second secret information are identical secret information for identical groups **[i.e., the group of encrypted application secrets associated with the user is referred to as a "keychain." Each keychain is assigned a public/private key pair, with all secrets in the keychain being encrypted with the public key. The user may be associated with one or more keychains, each of which may be further associated with different secrets (e.g. first secret, second secret, etc...). Since these secrets correspond to application programs, the association of programs to keychains may be based upon various characteristics, such as the user's rights with respect to the programs. Furthermore, each application program may be accessible by the same or different users so that, e.g., those users having the same access rights for a program may utilize the same keychain containing each user's secrets for the programs (column 3, lines 40-53 of Mashayekhi). Furthermore, referring to Figure 1, a distributed data processing network system 100 includes a plurality of computer nodes, such as user nodes 102a-n and various server nodes 104a-n, interconnected by a communications medium 106. The user node, e.g., a workstation 102a, is a computer generally configured for use by one user at a time, whereas each server 104 is a computer resource running specialized software applications and services, typically for use by many users. In general,**

each of the computer nodes includes memory means 108 for storing software programs and data structures associated with the cryptographic methods and techniques described herein (colùmn 4, line 61-67 through column 5, lines 1-5 of Mashayekhi)].

ii. Although Mashayekhi does address the authentication processes and a certificate authority (CA) for cryptographically binding the public key and the user name in a signed "certificate", Mashayekhi does not explicitly mention:

(1) performs said authentication by confirming that said issuance side processed value and said verification side processed value coincide.

iii. Ohashi teaches:

(1) If the encrypted Res' coincides with Res, a user certificate Cert and an authentication information AuInfo are issued for the smart card 10. Contents of the issued user certificate Cert and authentication information AuInfo are indicated in Figure 11 as an example **(column 13, lines 6-10 of Ohashi).**

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the coincidence of issuance and verification of a certification used in Ohashi's authentication processes into Mashayekhi's distributed network system in order to confirm that a user who requests network services or communications (hereinafter called as a network user) is a legitimate user, it is necessary at the network side to authenticate this user **(column 1, lines 10-13 of Ohashi)**.

v. The ordinary skilled person would have been motivated to:

(1) have applied the coincidence of issuance and verification of a certification used in Ohashi's authentication processes into Mashayekhi's distributed network system for identifying a user by network when the user intends to get network services **(column 1, lines 4-6 of Ohashi).**

vi. Although the combination of teaching between Mashayek and Ohashi teaches the claimed subject matter as described above, they are silent about grouping of certificate. On the other hand, Hamann teaches:

(1) An embodiment of the new certificate type is the group certificate. The group certificate is particularly suitable where several keys are to be issued at the same time for the same user by the same certification instance. By means of the group certificate, all redundant data elements are eliminated and all data elements for a set of several keys subject to certification are grouped into one certificate **(column 2, lines 33-39 of Hamann).**

vii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the teaching of Hamann into the combination of teaching between Mashayek and Ohashi for reducing the memory requirement, and for handling of the certificates is simplified for the communication partners **(column 2, lines 39-40 of Hamann).**

viii. The ordinary skilled person would have been motivated to:

(1) have modified the teaching of Hamann into the combination of teaching between Mashayek and Ohashi which can be transmitted fast to the various communication partners and results in reduced memory requirement on the storage media **(column 2, lines 21-23 of Hamann).**

b. *Referring to claim 3:*

i. Mashayekhi further teaches:

(1) wherein said cryptographic function is a hash function **[i.e., a user logs into the workstation with the user's password and the workstation derives a secret, non-complimentary, encryption key by applying a known hash algorithm to the password (column 2, lines 5-8 of Mashayekhi)].**

c. *Referring to claims 4-6:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

d. *Referring to claims 7, 18:*

i. These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

f. *Referring to claim 10:*

i. Mashayekhi further teaches:

(1) wherein it cooperates with a unique ID generation means provided in said client, and the unique ID generation means generates an authentication ID for mutual authentication between said client and said server, contains the authentication ID in said group certificate, and transmits the same to said server **[i.e., the flexible association of users, keychains and application secrets enables each user to have its own unique user identity and application secret for every application on the network. Thus, knowledge of one application secret does not compromise the security of all remaining application secrets associated with the user (column 4, lines 20-25). In addition, for every valid network user, the attributes of user object 302 include a login public/private key pair and a secret (e.g., the hash of the password). The user object 302 is accessed by the NDS to initially authenticate the user when the user logs on to the network. An application object 306 includes, for an associated application program, a program name, a list of users that have authority to access the program, and an application program identifier (ID). The program name attribute is a unique descriptive term that identifies the application program. The ID is a unique character string typically supplied by the application manufacturer that identifies the application program. However, the present invention reserves a pre-assigned range of IDs for programs that have no IDs assigned to them by their manufacturer. In the preferred embodiment of the present invention, the ID is an ASN.1 (abstract syntax notation; a CCITT/ISO standard) compliant identifier defined as a "Free Form Identifier." (column 6, lines 21-39 of Mashayekhi)].**

ii. Although the combination of teaching between Mashayek and Ohashi teaches the claimed subject matter as described above, they are silent about grouping of certificate. On the other hand, Hamann teaches:

(1) An embodiment of the new certificate type is the group certificate. The group certificate is particularly suitable where several keys are to be issued at the same time for the same user by the same certification instance. By means of the group certificate, all redundant data elements are eliminated and all data

elements for a set of several keys subject to certification are grouped into one certificate **(column 2, lines 33-39 of Hamann).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the teaching of Hamann into the combination of teaching between Mashayek and Ohashi for reducing the memory requirement, and for handling of the certificates is simplified for the communication partners **(column 2, lines 39-40 of Hamann).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the teaching of Hamann into the combination of teaching between Mashayek and Ohashi which can be transmitted fast to the various communication partners and results in reduced memory requirement on the storage media **(column 2, lines 21-23 of Hamann).**

g. *Referring to claims 11, 21:*

i. These claims have limitations that is similar to those of claim 10 and section (3) of claim 1, thus they are rejected with the same rationale applied against claim 10 and section (3) of claim 1 above.

h. *Referring to claim 12:*

i. Mashayekhi further teaches:

(1) wherein it cooperates with an encryption processing unit provided in said client, and the encryption processing unit establishes an encryption session from the client to said server with said temporary password as an encryption key **[i.e., a user logs into the workstation with the user's password and the workstation derives a secret, non-complimentary, encryption key by applying a known hash algorithm to the password (column 2, lines 5-8 of Mashayekhi)].**

i. *Referring to claim 13:*

i. Mashayekhi further teaches:

(1) wherein provision is made of a log file for recording the log of the session according to each said remote processing request for each of said users, and supervision of each user is performed based on the log **[i.e., referring to**

Figure 1, in general, each of the computer nodes includes memory means 108 for storing software programs and data structures associated with the cryptographic methods and techniques (column 5, lines 1-5 of Mashayekhi)].

j. *Referring to claims 14, 24:*

i. Mashayekhi further teaches:

(1) wherein said temporary password for every said session is included in said log and thereby to identify the sessions **[i.e., once the user is authenticated by the directory services on the network, and is then given access to the network, the user attempts to access either network-based services or applications. For example, the user may attempt to log into a different network or access a different operating system (e.g., accessing a DCE-based Unix server) or access applications such as Lotus Notes or Novell GroupWise. Generally, each of these entities includes a component referred to as an authentication agent that maintains the user's identity (ID) and secrets (e.g., passwords) (column 2, lines 19-28 of Mashayekhi)].**

k. *Referring to claim 23:*

i. These claims have limitations that is similar to those of claim 13, thus they are rejected with the same rationale applied against claim 13 above.

l. *Referring to claim 17:*

i. Mashayekhi further teaches:

(1) wherein provision is made of a user-group mapping storage means, and in the user-group mapping storage means, a plurality of different groups can be assigned for one said user **[i.e., the novel distributed service 201 comprises an exchange controller 207 coupled to an authentication database 204 containing a group of encrypted application secrets associated with the user (column 5, lines 60-64). Furthermore, the authentication database 204 is preferably a novel secure database containing groups of application secrets for predetermined application programs. Each group of application secrets, referred to as a "keychain", is assigned a public/private key pair by the KG 218 when the keychain is created. The database 204 also contains user objects which**

associate a given user with one or more keychains. The database API 206 manages the authentication database 204 in response to queries generated by workstation API 214. (column 6, lines 3-11)].

m. *Referring to claim 22:*

i. This claim has limitations that is similar to those of claim 12, thus it is rejected with the same rationale applied against claim 12 above.

o. *Referring to claim 25:*

i. This claim has limitations that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

p. *Referring to claim 27:*

i. Mashayekhi further teaches:

(1) wherein it cooperates with a group certificate temporary storing unit provided in said server, and, when the assignment of a plurality of different groups is enabled for one said user, it verifies said group certificates received from said client, stores them in the group certificate temporary storing unit, and switches and uses the stored group certificates in accordance with said predetermined authorization necessary for the request with respect to the following remote processing requests **[i.e., Figure 2 discloses a certificate storage server (CSS) node for storing certificate (column 4, lines 47-48). Furthermore, the workstation and server nodes may be configured as a distributed authentication service 201 that automates an authentication exchange between a user interface 112 200. The novel distributed service 201 comprises an exchange controller 207 coupled to an authentication database 204 containing a group of encrypted application secrets associated with the user. The controller 207, in turn, comprises an application program interface (API) that is distributed among user workstations (i.e., workstation API 214) and the authentication database (i.e., the database API 206). Illustratively, both the database API and authentication database reside in a network directory services (NDS) system (column 5, lines 57-67 through column 6, lines 1-2)].**

q. *Referring to claim 28:*

i. This claim has limitations that is similar to those of claim 27, thus it is rejected with the same rationale applied against claim 27 above.

5. Claims 8, 9, 15-16, 19-20, 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mashayekhi (US 5,818,936), further in view of Ohashi et al (US 5,761,309), further in view of Perlman (US 5,892,828), and further in view of Hamann (US 6,981,147 B1).

a. *Referring to claims 8, 9:*

i. Although the combination of teaching between Mashayek and Ohashi teaches the claimed subject matter as described above, and Mashayekhi briefly teaches the hash algorithm, however the detail of the hash algorithm has not been shown precisely. On the other hand, Perlman teaches:

(1) Perlman's invention generally relates to a technique for verifying the presence of a user to applications stored on a distributed network system using a single password. Briefly, the technique generally comprises computing a one-way hash value of the password that is initially provided by the user to a workstation during a login procedure **(column 3, lines 34-39).** Referring to Figure 4 for the sequence of steps for dynamically verifying the presence of a user when authenticating the user to various services and applications in a distributed network system.

ii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly show the sequence of steps in hash algorithm for authentication processes as in Perlman for verifying the identity of a user of a distributed network system prior to allowing the user access to system resources and applications is referred to as authentication **(column 1, lines 20-22 of Perlman).**

iii. The ordinary skilled person would have been motivated to:

(1) clearly show the sequence of steps in hash algorithm for authentication processes as in Perlman since cryptography is often used to preserve the confidentiality of the transmitted password when authenticating the user to remote applications. Furthermore, a well-known cryptographic technique used to perform

remote authentication is public key cryptography, wherein a public key system may be used in such a way as to ensure that information being transmitted cannot be understood by an eavesdropper, as well as to ensure the authenticity of the sender of the information **(column 1, lines 40-54 of Perlman).**

iv. Besides the combination of teaching between Mashayek, Ohashi, and Perlman teaches the claimed subject matter as described above, they are silent about grouping of certificate. On the other hand, Hamann teaches:

(1) An embodiment of the new certificate type is the group certificate. The group certificate is particularly suitable where several keys are to be issued at the same time for the same user by the same certification instance. By means of the group certificate, all redundant data elements are eliminated and all data elements for a set of several keys subject to certification are grouped into one certificate **(column 2, lines 33-39 of Hamann).**

v. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the teaching of Hamann into the combination of teaching between Mashayek and Ohashi for reducing the memory requirement, and for handling of the certificates is simplified for the communication partners **(column 2, lines 39-40 of Hamann).**

vi. The ordinary skilled person would have been motivated to:

(1) have modified the teaching of Hamann into the combination of teaching between Mashayek and Ohashi which can be transmitted fast to the various communication partners and results in reduced memory requirement on the storage media **(column 2, lines 21-23 of Hamann).**

b. *<u>Referring to claim 15:</u>*

i. This claim has limitations that is similar to those of claims 8 and 10, thus it is rejected with the same rationale applied against claims 8 and 10 above.

c. *<u>Referring to claim 16:</u>*

i. This claim has limitations that is similar to those of claims 9 and 10, thus it is rejected with the same rationale applied against claims 9 and 10 above.

d. *Referring to claim 19:*

i. This claim has limitations that is similar to those of claims 3 and 8, thus it is rejected with the same rationale applied against claims 3 and 8 above.

e. *Referring to claim 20:*

i. This claim has limitations that is similar to those of claim 9 and section (3) of claim 1, thus it is rejected with the same rationale applied against claim 9 and section (3) of claim 1 above.

f. *Referring to claim 26:*

i. This claim has limitations that is similar to those of claims 9 and 10, thus it is rejected with the same rationale applied against claims 9 and 10 above.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT

April 14, 2006